Procedimiento de desconexión de equipos de la red de datos por motivos de seguridad UC3M

Introducción

El objeto de la presente propuesta es dotar al Área de Seguridad y Comunicaciones (ASyC) del Servicio de Informática y Comunicaciones (SdIC) de un procedimiento ágil, preciso y consensuado para limitar la difusión de virus y gusanos informáticos y otro tipo de incidentes relacionados con la seguridad informática a través de la red de la universidad.

Cada día surgen nuevos programas que amenazan la seguridad de los datos y aplicaciones instaladas en los ordenadores. Estos programas utilizan las redes de comunicación para propagarse, por lo que tanto el ordenador del despacho y/o aulas informáticas como el de casa (si se utiliza la conexión a Internet) están amenazados. Además, estos programas pueden generar problemas en el resto de equipos conectados a la red.

Como consecuencia de una infección por un virus o gusano, nuestro ordenador se ralentiza y la conexión a Internet o con los servidores de la universidad se degrada. En determinadas ocasiones no sería posible acceder a algunos servicios de red.

Además, el hecho de mantener un ordenador infectado o asaltado conectado a Internet implica un riesgo de infección por gusanos /virus y también la posibilidad de que un intruso acceda a dicho ordenador y lo utilice como plataforma para atacar los sistemas informáticos de la universidad o de terceros.

Fundamentación de la propuesta

El artículo 9 del Reglamento del Servicio de Informática[1] establece:

"...En el supuesto de que un usuario, sistema, dispositivo o medio pusiera en grave peligro la seguridad del Sistema General Informático de la Universidad, el Director del Servicio podrá suspender la prestación de servicios desde el sistema, informando, dentro de las 24 horas siguientes, al Presidente del Consejo Informático y al usuario afectado de esta medida, así como de las demás propuestas para su subsanación. La suspensión deberá ser confirmada o levantada por el Presidente del Consejo, extinguiéndose, además, en todo caso automáticamente a) como efecto de la subsanación efectiva y comprobada de los problemas detectados, y b) por el transcurso de 72 horas sin práctica de la comunicación de la medida suspensiva al Presidente del Consejo. El mantenimiento de la medida de suspensión requerirá la apertura de los procedimientos que en cada caso procedan para depurar las responsabilidades a que pueda haber lugar."

De lo que se deduce que el SdIC tiene las siguientes obligaciones:

- Velar por la seguridad del Sistema General Informático de la Universidad.
- Notificar al usuario y al Director del SdIC de las suspensiones del servicio según se realicen y de las acciones que deben emprenderse para subsanar el problema existente.

Ámbito de aplicación

El siguiente procedimiento debe aplicarse a todos aquellos equipos informáticos y de comunicaciones que empleen la red de la Universidad. Esto incluye, pero no se limita a:

- Ordenadores propiedad de la universidad ubicados en despachos y laboratorios.

- Ordenadores personales conectados directamente a la red de la universidad
- Desde las rosetas de conexión de los despachos y laboratorios.
- Mediante conexión inalámbrica (WiFi)
- Mediante el acceso telefónico proporcionado por SdIC.
- Cualquier otro medio de conexión departamental que permita el acceso a la red de la universidad.
- Ordenadores conectados a Internet a través de proveedores de acceso (ADSL, Tarifa Plana, etc) que emplean el acceso mediante red privada virtual (VPN).

Definiciones

Actualización o Parche: Archivo o conjunto de archivos, que corrige un fallo de seguridad existente en una aplicación informática.

ADSL: Tecnología de conexión a Internet con elevado caudal de acceso, popularizada gracias a las ofertas de tarifa plana de las operadoras.

Antivirus: Programa capaz de detectar la presencia de un virus y neutralizar sus efectos.

Dirección IP: Identificador compuesto por cuatro números (de tres o menos cifras), que permite designar de forma unívoca un ordenador conectado a Internet.

Dirección MAC o de enlace: Identificador compuesto por 6 números, asociado a las tarjetas de conexión a la red.

Escaneo: Técnica empleada por los intrusos para determinar los servidores de una organización (escaneo de equipos) o los servicios activos de un ordenador (escaneo de puertos).

Gusano: Programa malicioso, que utiliza la red de comunicación para atacar a otros ordenadores y se copia aprovechando vulnerabilidades en el sistema operativo o en las aplicaciones instaladas.

Puerta trasera: Servicio instalado por un intruso para garantizarse el acceso al sistema, aun cuando el administrador instale todos las actualizaciones del sistema.

RADIUS: Servicio de autenticación, empleado para validar la identidad del usuario en los accesos telefónico y red privada virtual (VPN).

Red Privada Virtual: Técnica que permite, manteniendo la conexión con nuestro proveedor habitual, acceder a los servicios de la red como si el ordenador se encontrase conectado a otra red, por ejemplo la red de la universidad.

Service Pack: Conjunto de parches agrupados para facilitar la instalación por parte del usuario.

Troyano: Programa que a primera vista realiza una función (por ejemplo visualizar una imagen), pero que además realiza otras funciones no visibles (por ejemplo instala programas maliciosos o permite acceso remoto al ordenador).

Virus: Programa malicioso, similar al gusano, pero que modifica ("infecta") un programa existente para asegurarse la transmisión de un ordenador a otro.

VPN: Véase Red Privada Virtual.

Vulnerabilidad: Fallo de diseño o programación en una aplicación informática que da lugar a un problema de seguridad.

WiFi: Técnica de conexión a la red que emplea ondas de radio para la transmisión de datos, en lugar de cables de cobre o fibra óptica.

Procedimiento de desconexión

Fase 1: Detección de equipos comprometidos

El personal del SdIC, empleando herramientas para la detección de intrusiones, considerará que un ordenador se encuentra comprometido si detecta un comportamiento anormal en el uso de la red.

Entre estos comportamientos anómalos se incluyen, pero no se limitan a:

- Escaneo de equipos y/o puertos hacia ordenadores situados dentro y fuera de la red de la universidad.
- Generación de tráfico similar al generado por virus, gusanos y otros programas maliciosos.
- Intentos de explotación de vulnerabilidades conocidas, publicadas por los fabricantes, organismos internacionales y empresas de seguridad informática.

Como resultado de esta fase se obtiene la dirección IP del equipo presuntamente comprometido.

Fase 2: Determinación de la ubicación del equipo comprometido

El personal de SdIC empleando herramientas de gestión propias puede determinar en la mayoría de los casos la siguiente información, asociada a una dirección IP correspondiente a un ordenador que se encuentre dentro del ámbito de aplicación de este procedimiento:

- Dirección MAC o de enlace.
- Roseta de conexión.
- Dependencia en la que se ubica dicha roseta.

Como resultado de esta fase, se puede determinar si el equipo se ha conectado directamente a la red de la universidad, a través de la red inalámbrica, a través de la red virtual (VPN) o a través del acceso telefónico proporcionado por el SdIC. Excepto en el primer caso, es posible determinar el usuario que utilizó el servicio.

Fase 3: Desconexión del equipo comprometido

El personal de SdIC, procederá a suspender el servicio de conexión al equipo comprometido, pudiendo emplear para ello varios mecanismos, que incluyen, pero no se limitan a:

- Deshabilitar la transmisión de datos en la roseta de conexión del equipo comprometido.
- Bloquear el tráfico con origen o destino a la dirección MAC del equipo comprometido.
- Bloquear el tráfico con origen o destino a la dirección IP del equipo comprometido.

Estos mecanismos no son efectivos para aquellos equipos que emplean red inalámbrica, red privada virtual o el acceso telefónico proporcionado por el SdIC, que se determinan en la fase 4, punto 4.

Fase 4: Determinación del usuario asociado al equipo comprometido

El personal de SdIC, procederá a obtener información asociada a la dependencia en la que se encuentra el equipo comprometido. Como resultado de ello pueden obtenerse los siguientes resultados:

- La dependencia obtenida en la fase 2 corresponde al despacho asignado a un usuario.
- La dependencia obtenida en la fase 2 corresponde a un laboratorio o aula departamental.
- La dependencia obtenida en la fase 2 no corresponde a ningún laboratorio o aula departamental.
- Usuario que estableció la conexión, aplicable a aquellos equipos que emplean red inalámbrica, red privada virtual o el acceso telefónico proporcionado por el SdIC. En este caso el personal de SdIC procederá a inhabilitar el acceso en el servidor RADIUS.

Como resultado de esta fase, pueden obtenerse uno de los siguientes resultados:

- Usuario asociado al equipo comprometido.
- Departamento/Servicio asociado al equipo comprometido.
- Carencia de información sobre el departamento o persona asociada al equipo comprometido.

Fase 5: Notificación de la desconexión y medidas para subsanar el compromiso

El personal del SdIC, notificará mediante un mensaje de correo electrónico la desconexión del equipo comprometido a:

- Usuario o persona de contacto del departamento o servicio asociado al equipo comprometido. En el caso de laboratorios, aulas departamentales y otras dependencia no asociadas a personas en las bases de datos corporativas, el mensaje será enviado a la persona de contacto del departamento y/o al director del departamento.
- Director del SdIC.
- Centro de Atención a Usuarios del campus en el que se encuentre el equipo comprometido.

El mensaje incluirá el motivo de la desconexión y las pautas a seguir para subsanar el compromiso del equipo.

Adicionalmente, el SdIC mantendrá la información referente a desconexiones en web con un servicio de búsqueda por usuario, dirección IP y/o despacho.

Fase 6: Subsanación del compromiso

Equipos propiedad de la universidad

En el caso de equipos de la universidad con la instalación homologada por el SdIC, el Centro de Atención a Usuarios se encargará del proceso de subsanación, solicitando internamente el restablecimiento de la conexión al equipo comprometido.

Equipos privados

En el caso de equipos privados, es responsabilidad del usuario la subsanación del problema, empleando para ello los medios y proveedores que estime convenientes. El SdIC tiene publicada en Web información sobre la realización de este proceso de forma autónoma. Además conoce empresas que proporcionan este servicio para recomendarlas al usuario.

Una vez subsanado el compromiso, el usuario solicitará al Centro de Atención a Usuarios elrestablecimiento de la conexión.

Fase 7: Reconexión

El personal de SdIC procederá a restaurar la conexión al equipo comprometido tan pronto como tenga solicitud de ello, excepto en caso de reincidencia de equipos privados. Para ello el Consejo Informático o en su defecto el director del SdIC establecerán penalizaciones en el proceso de reconexión, teniendo en cuenta para ello factores tales como:

- Número de desconexiones realizadas al usuario.
- Tiempo transcurrido desde la última desconexión del usuario.

Condicionantes para el correcto funcionamiento del procedimiento propuesto

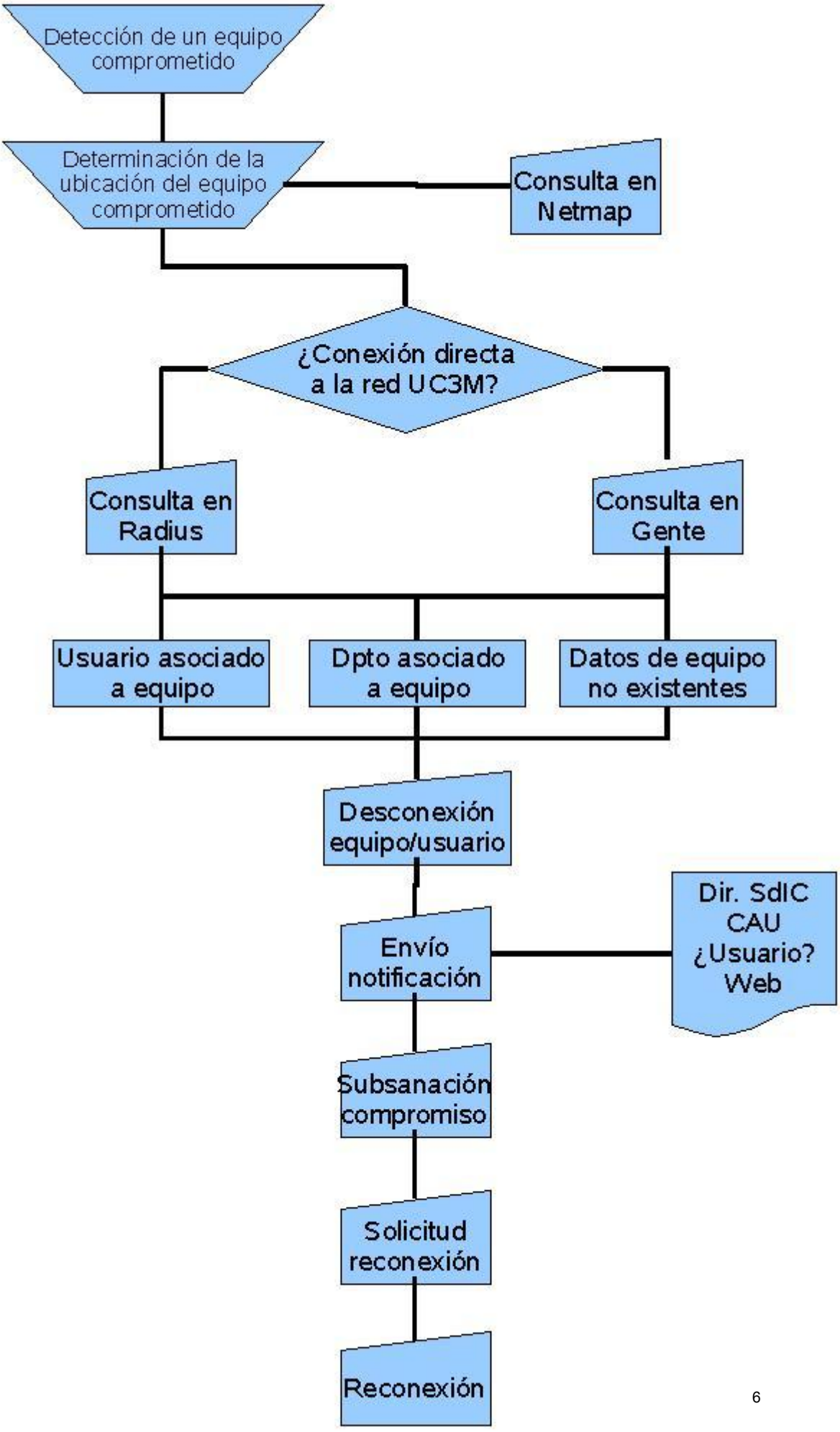
El requisito más difícil de llevar a cabo del artículo 9 del Reglamento del Servicio de Informática es
asociar el equipo comprometido con el usuario responsable de dicho equipo. Para poder cumplirlo
son necesarias dos condiciones:

- Los datos correspondientes a la asignación de despachos almacenados en las bases de datos corporativas deben mantenerse actualizados, siendo esta labor realizada por las secretarías de los departamentos y por los propios usuarios de los servicios. Es posible cambiar los datos referentes al despacho y/o teléfono en el Directorio Electrónico, seleccionando "Directorio" en las opciones de la cabecera de Campus Global, junto a la opción "Salir".
- Los departamentos deben facilitar una lista de laboratorios/aulas departamentales que se encuentran a su cargo y la persona de contacto para incidentes de seguridad.

Referencias:

1. Reglamento del Servicio de Informática, http://www.uc3m.es/uc3m/gral/IG/NOR/norm502.html, 17 de junio de 1.997

Anexo I: Diagrama de flujo del proceso


Detección de un equipo comprometido
Determinación de la ubicación del equipo comprometido
Consulta en Netmap
¿Conexión directa a la red UC3M?
Consulta en Radius
Consulta en Gente
Usuario asociado a equipo
Dpto asociado a equipo
Datos de equipo no existentes
Desconexión equipo/usuario
Envío notificación
Dir. SdIC
CAU
¿Usuario?
Web
Subsanación compromiso
Solicitud reconexión
Reconexión

Anexo 2: Modelo de notificación

Estimado Nombre y Apellidos
El Servicio de Informática ha detectado que el ordenador 163.117.x.y, ubicado en el
despacho a.b.c.d probablemente ha sido infectado por el virus VIRUS. Por ello y para
evitar su propagación entre el resto de equipos de la comunidad universitaria nos hemos
visto en la obligación de bloquear su acceso a la red de la universidad.
Si el equipo afectado es personal (no es propiedad de la Universidad), puede
encontrar información sobre como instalar el anti-virus corporativo y
actualizar su equipo en la siguiente página Web:
http://unamuno.uc3m.es/cau-cg/seguridad/seguridad.html
Si el equipo afectado es propiedad de la Universidad, el servicio de soporte
informático se hará cargo de las operaciones de desinfección y puesta a
punto del equipo.
* Equipos de Tercer Ciclo: Persona de contacto en Tercer Ciclo, correo@persona_de_contacto
(15.1.35)
* Servicio de Biblioteca, para los equipos de préstamo de biblioteca.
* Restantes equipos de la universidad: Centro de Atención a Usuarios.
IMPORTANTE: La medida aplicada sólo afecta a la conexión a red del equipo afectado,
pudiendo leer el correo y acceder a otros servicios de red desde cualquier otro
ordenador.
Atentamente. Servicio de Informática y Comunicaciones

Centro de Atención a Usuarios Campus de Colmenarejo: 1269
Campus de Leganés: 9980
Campus de Getafe: 9523

Servicio de Informática y Comunicaciones (SdIC) 7 Área de Seguridad y Comunicaciones (ASyC)